UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/849,403	05/07/2001	Sam Shiaw-Shiang Jiang	ASTP0012USA	9459

7590   04/26/2004

NAIPO (North America International Patent Office)
P.O. Box 506
Merrifield, VA 22116

EXAMINER
BAUM, RONALD

ART UNIT	PAPER NUMBER
2136	8

DATE MAILED: 04/26/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
Office Action Summary	09/849,403	JIANG, SAM SHIAW-SHIANG
	Examiner	Art Unit
	Ronald Baum	2136

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date <u>5</u>.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

U.S. Patent and Trademark Office

PTOL-326 (Rev. 1-04)   **Office Action Summary**   Part of Paper No./Mail Date 8

DETAILED ACTION

1.   Claims 1- 27 are pending for examination.

2.   Claims 1- 27 are rejected.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

3.   Claims 1-27 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. In claims 1,11,20 and 25 (and by dependency the associated dependent claims), the first and second stations comprise the various elements as recited in the claim language including "a [first / second] hyper frame *number* (HFN) ...". A *number* per se is non-statutory subject matter. Further, claim 20 (and by dependency the associated dependent claims), recites "A data structure..." which is also non-statutory subject matter (i.e., a data structure may be embodied on a computer readable media). For the sake of applying art, the examiner assumes the HFN is stored in the system, in a memory storage (means), and the "data structure" is computer readable media embodied.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4.   Claims 1-27 are rejected under 35 U.S.C. 102(b) as being anticipated by Finkelstein et al,

U.S. Patent 5,319,712.

5.   As per claim 1; "A method for synchronizing a ciphering key change in a wireless

communications system, the wireless communications system comprising: a first station capable

of receiving a security mode command to effect a ciphering change, and capable of receiving

encrypted layer 2 protocol data units (PDUs), each received PDU being sequentially identified

by an n-bit frame number (FN), the first station comprising: a first m-bit hyper frame number

(HFN); and a decryption unit capable of decrypting received PDUs according to at least a first

ciphering key, the first HFN, and the FN of each received PDU; and a second station capable of

transmitting the security mode command, and capable of transmitting encrypted PDUs, the

second station comprising: a second m-bit HFN; and an encryption unit capable of encrypting

transmitted PDUs according to at least the first ciphering key, the second HFN, ,and an FN

associated with each transmitted PDU; the method comprising: the second station determining an

activation time at which a ciphering key change is to occur [col. 1,lines 52-64, col. 2,lines 4-13,

col. 3,lines 20-58]; the second station composing the security mode command, the security mode

command comprising a switching FN corresponding to the activation time, and x least-

significant bits (LSBs) from the second HFN corresponding to the activation time [col. 3,lines

59-col. 4,line 32]; the second station transmitting the security mode command [col. 2,lines 30-44

]; the first station receiving the security mode command; the first station utilizing the switching

FN and the x LSBs from the second HFN contained in the security mode command to obtain an

application time [col. 4,lines 48-col. 5,line 33]; and the first station using the first ciphering key

to decrypt PDUs with FNs sequentially prior to the application time, and using a second

ciphering key to decrypt PDUs with FNs sequentially on or after the application time [col. 1,lines 65-col. 2,line 14, col. 5,lines 33-65].".

6.   Claim 2 *additionally recites* the limitation that; "[The method of claim 1] wherein the first station increments the first HFN by a predetermined value on detection of roll-over of an FN of a received PDU.". The teachings of Finkelstein et al suggest such limitations (col. 3,lines 1-col. 2,line 32, col. 4,lines 48-col. 5,line 6, figure 1 and accompanying description);

7.   Claim 3 *additionally recites* the limitation that; "[The method of claim 1] wherein the second station increments the second HFN by a predetermined value on detection of roll-over of an FN of a transmitted PDU.". The teachings of Finkelstein et al suggest such limitations (col. 3,lines 1-col. 2,line 32, col. 4,lines 48-col. 5,line 6, figure 1 and accompanying description).

8.   Claim 4 *additionally recites* the limitation that; "[The method of claim 1] wherein the first HFN and the second HFN are synchronized.". The teachings of Finkelstein et al suggest such limitations (col. 3,lines 1-col. 2,line 32, col. 4,lines 48-col. 5,line 6, figure 1 and accompanying description).

9.   Claim 5 *additionally recites* the limitation that; "[The method of claim 4] wherein the activation time corresponds to a second HFN/FN sequence pair for a crossover PDU, the crossover PDU being the sequentially earliest PDU encrypted using the second ciphering key, and the application time corresponds to a synchronized first HFN/FN sequence pair for a corresponding received PDU.". The teachings of Finkelstein et al suggest such limitations (col. 1,lines 65-col. 2,line 14, col. 4,lines 33-col. 5,line 65).

10.   Claim 6 *additionally recites* the limitation that; "[The method of claim 5] wherein the switching FN is the FN of the crossover PDU, and the x LSBs are extracted from the second

HFN corresponding to the crossover PDU.". The teachings of Finkelstein et al suggest such limitations (col. 4,lines 48-col. 5,line 33).

11.   Claim 7 *additionally recites* the limitation that; "[The method of claim 1] wherein the activation time is equal to the application time.". The teachings of Finkelstein et al suggest such limitations (col. 1,lines 65-col. 2,line 14, col. 4,lines 48-col. 5,line 65).

12.   Claim 8 *additionally recites* the limitation that; "[The method of claim 1] wherein x is greater than or equal to 2.". The teachings of Finkelstein et al suggest such limitations (col. 4,lines 48-col. 5,line 33, figure 1 and accompanying description).

13.   Claim 9 *additionally recites* the limitation that; "[The method of claim 1] wherein x is equal to m.". The teachings of Finkelstein et al suggest such limitations (col. 4,lines 48-col. 5,line 33, figure 1 and accompanying description).

14.   Claim 10 *additionally recites* the limitation that; "[The method of claim 1] wherein the first station compares the x LSBs from the second HFN contained in the security mode command to determine a cyclical positioning of the switching FN within the first HFN.". The teachings of Finkelstein et al suggest such limitations (col. 1,lines 65-col. 2,line 14, col. 4,lines 48-col. 5,line 65, figure 1 and accompanying description).

15.   As per claim 11; "A wireless communications system [This claim is a apparatus (system) claim for the method claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection] comprising: a first station capable of receiving encrypted layer 2 protocol data units (PDUs), and capable of receiving a security mode command, the first station comprising: a receiving buffer for storing received PDUs, the first station associating a sequentially ordered n-bit frame number (FN) and an m-bit hyper frame number (HFN) with each received PDU; an

extraction unit for obtaining an application time from a switching FN and x least significant bits (LSBs) of a second HFN, the switching FN and the x LSBs of the second HFN contained in the security mode command; a first ciphering key; a second ciphering key; and a decryption unit for decrypting the received PDUs, the decryption unit using the first ciphering key to decrypt any received PDU with an HFN/FN pair that is sequentially before the application time, and using the second ciphering key to decrypt any received PDU with an HFN/FN pair that is sequentially on or after the application time.".

16.   Claim 12 *additionally recites* the limitation that; "[The system of claim 11] further comprising [This claim is a apparatus (system) claim for the method claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection] a second station capable of transmitting the security mode command, and capable of transmitting the encrypted PDUs; wherein PDUs that are sequentially before the application time are encrypted using the first ciphering key, and PDUs sequentially on or after the application time are encrypted using the second ciphering key.".

17.   Claim 13 *additionally recites* the limitation that; "[The system of claim 12] wherein the HFN of each received PDU is synchronized with a co-responding HFN on the second station for each PDU transmitted by the second station.". The teachings of Finkelstein et al suggest such limitations (This claim is a apparatus (system) claim for the method claim 4 above, and is rejected for the same reasons provided for the claim 4 rejection).

18.   Claim 14 *additionally recites* the limitation that; "[The system of claim 13] wherein the second station comprises an encryption unit capable of generating an activation time, the activation time corresponding to an HFN/FN sequence pair for a crossover PDU, the crossover

PDU being the sequentially earliest PDU encrypted by the encryption unit using the second

ciphering key, and the application time corresponds to a synchronized HFN/FN sequence pair for

a corresponding PDU received by the first station.". The teachings of Finkelstein et al suggest

such limitations (This claim is a apparatus (system) claim for the method claim 1 above, and is

rejected for the same reasons provided for the claim 1 rejection).

19.   Claim 15 *additionally recites* the limitation that; "[The system of claim 14] wherein the

switching FN is the FN of the crossover PDU, and the second HFN is the HFN of the crossover

PDU.". The teachings of Finkelstein et al suggest such limitations (col. 3,lines 1-col. 2,line 32,

col. 4,lines 48-col. 5,line 6, figure 1 and accompanying description).

20.   Claim 16 *additionally recites* the limitation that; "[The system of claim 14] wherein the

activation time is equal to the application time.". The teachings of Finkelstein et al suggest such

limitations (col. 1,lines 65-col. 2,line 14, col. 4,lines 48-col. 5,line 65).

21.   Claim 17 *additionally recites* the limitation that; "[The system of claim 11] wherein the

first station increments the HFN associated with a first PDU by a predetermined value on

rollover of the FN associated with the first PDU.". The teachings of Finkelstein et al suggest

such limitations (This claim is a apparatus (system) claim for the method claim 2 above, and is

rejected for the same reasons provided for the claim 2 rejection).

22.   Claim 18 *additionally recites* the limitation that; "[The system of claim 11] wherein x is

greater than or equal to 2.". The teachings of Finkelstein et al suggest such limitations (col.

4,lines 48-col. 5,line 33, figure 1 and accompanying description).

23.   Claim 19 *additionally recites* the limitation that; "[The system of claim 11] wherein x is

equal to m.". The teachings of Finkelstein et al suggest such limitations (col. 4,lines 48-col.

5,line 33, figure 1 and accompanying description).

24.   As per claim 20; "A data structure [For the purpose of applying art, this claim is the

stored memory (means), and the "data structure" is computer readable media embodied claim

(see 101' rejection above) for the method claim 1 above, and is rejected for the same reasons

provided for the claim 1 rejection] for use in a wireless communications system to synchronize a

ciphering key change in the wireless communications system, the wireless communications

system comprising: a first station capable of receiving encrypted layer 2 protocol data units

(PDUs), assigning a first n-bit frame number (FN) and a first m-bit hyper frame number (HFN)

to each received PDU to generate a first HFN/FN pair for each received PDU, and decrypting

each received PDU according to the first HFN/FN pair, an application time, a first ciphering key,

and a second ciphering key, the first station using the first ciphering key if the first HFN/FN pair

is sequentially before the application time, and using the second ciphering key if the first

HFN/FN pair is sequentially on or after the application time; and a second station capable of

transmitting the encrypted PDUs, the second station assigning a second n-bit FN and a second m-

bit HFN to each PDU to be transmitted to generate a second HFN/FN pair for each PDU to be

transmitted, and encrypting each PDU to be transmitted according to the second HFN/FN pair,

an activation time, a third ciphering key, and a fourth ciphering key, the second station using the

third ciphering key if the second HFN/FN pair is sequentially before the activation time, and

using the fourth ciphering key if the second HFN/FN pair is sequentially on or after the

activation time; the data structure comprising: x least significant bits (LSBs) of a second HFN

corresponding to the activation time; and a switching FN corresponding to the activation time;

wherein the second station composes the data structure and transmits the data structure to the

first station to enable the first station to synchronize the application time with the activation

time.".

25.   Claim 21 *additionally recites* the limitation that; "[The data structure (For the purpose of

applying art, this claim is the stored memory (means), and the "data structure" is computer

readable media embodied claim (see 101' rejection above)) of claim 20] wherein the switching

FN is the FN of a second HFN/FN pair of a crossover PDU transmitted by the second station, the

crossover PDU being the sequentially earliest PDU encrypted using the fourth ciphering key, and

the x LSBs are extracted from the HFN of the second HFN/FN pair of the crossover PDU.". The

teachings of Finkelstein et al suggest such limitations (col. 1,lines 65-col. 2,line 14, col. 4,lines

33-col. 5,line 65).

26.   Claim 22 *additionally recites* the limitation that; "[The data structure (For the purpose of

applying art, this claim is the stored memory (means), and the "data structure" is computer

readable media embodied claim (see 101' rejection above) for the method claim 8 above, and is

rejected for the same reasons provided for the claim 8 rejection) of claim 20] wherein x is two.".

27.   Claim 23 *additionally recites* the limitation that; "[The data structure (For the purpose of

applying art, this claim is the stored memory (means), and the "data structure" is computer

readable media embodied claim (see 101' rejection above)) of claim 20] wherein the third

ciphering key is associated with the first ciphering key, and the fourth ciphering key is associated

with the second ciphering key.". The teachings of Finkelstein et al suggest such limitations (col.

1,lines 65-col. 2,line 14, col. 4,lines 33-col. 5,line 65).

28.   Claim 24 *additionally recites* the limitation that; "[The data structure (For the purpose of

applying art, this claim is the stored memory (means), and the "data structure" is computer

readable media embodied claim (see 101' rejection above)) of claim 23] wherein the third

ciphering key is identical to the first ciphering key, and the fourth ciphering key is identical to

the second ciphering key.". The teachings of Finkelstein et al suggest such limitations (col.

1,lines 65-col. 2,line 14, col. 4,lines 33-col. 5,line 65).

29.   As per claim 25; "A method for removing cyclical ambiguity of an n-bit identifying

frame number (FN) transmitted in a signaling message from a first station to a second station in a

wireless communications system, the identifying FN identifying a layer protocol data unit (PDU)

in a stream of PDUs, the first station comprising a first m-bit hyper frame number (HFN) that is

incremented by a first value upon detection of roll-over of an FN in the stream of PDUs, each

PDU in the stream of PDUs having an associated FN value and each FN value having an

associated HFN value, the method comprising: the first station placing the identifying FN into a

first field of a message; the first station placing x least significant bits (LSBs) from the HFN

value associated with the identifying FN in a second field of the message; and the first station

transmitting the message to the second station [col. 1,lines 52-64, col. 2,lines 4-13, col. 3,lines

20-58, col. 3,lines 59-col. 4,line 32]; wherein after reception of the message, the second station

uses the x LSBs of the second field to determine a cyclical position of the identifying FN [col.

1,lines 65-col. 2,line 14, col. 4,lines 48-col. 5,line 65].".

30.   Claim 26 *additionally recites* the limitation that; "[The method of claim 25] wherein x is

greater than or equal to two.". The teachings of Finkelstein et al suggest such limitations (col.

4,lines 48-col. 5,line 33, figure 1 and accompanying description).

31.   Claim 27 *additionally recites* the limitation that; "[The method of claim 25] wherein the

second station has a second HFN that is synchronized with the HFN of the first station, and the

second station uses the x LSBs of the second field to determine the cyclical position of the

identifying FN within the second HFN.". The teachings of Finkelstein et al suggest such

limitations (col. 1,lines 65-col. 2,line 14, col. 4,lines 48-col. 5,line 65).

Conclusion

32.   Any inquiry concerning this communication or earlier communications from examiner

should be directed to Ronald Baum, whose telephone number is (703) 305-4276. The examiner

can normally be reached Monday through Friday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Ayaz Sheikh, can be reached at (703) 305-9648. The Fax numbers for the

organization where this application is assigned are:

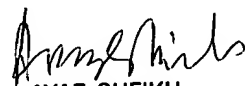After-final   (703) 746-7238

Official   (703) 746-7239

Non-Official/Draft   (703) 746-7246

Ronald Baum

Patent Examiner

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100